УДК 519.711

АЛГОРИТМ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ В СИСТЕМАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Ковальчук П.Р.

Національний авіаційний університет, м.Київ

Науковий керівник – Морозова І.В.,канд. техн. наук, доцент

Досліджується проблема оцінки ризиків кібербезпеки в організаціях. Кожна організація має свій унікальний набір ризиків безпеки і повинна використовувати власний підхід до оцінки цих ризиків. Проведення оцінки ризиків є складною частиною стратегії управління ризиками, але воно має багато переваг, таких як зменшення витрат, забезпечення базового рівня для організаційного ризику, підтримка потреби в програмі кібербезпеки та інші..

Кожна організація стикається зі своїм власним унікальним набором ризиків безпеки, і їй необхідно використовувати свій власний підхід до оцінки ризиків кібербезпеки.

Стандарти кібербезпеки та нормативні вимоги визнають, що різні компанії повинні використовувати різні підходи для захисту своїх інформаційних систем. Щоб захистити свої дані від кіберзлочинності та підвищити загальну безпеку, потрібна комплексна програма захисту інформаційних технологій.

Початок роботи з оцінки ризиків кібербезпеки є найскладнішою частиною стратегії управління ризиками. Спочатку розглянемо, хто повинен виконувати оцінку ризиків кібербезпеки, а також переваги її проведення. Усі організації, які використовують IT-інфраструктуру, повинні проводити оцінку ризиків кібербезпеки.

Однак деякі малі підприємства можуть мати обмежений бюджет або робочу силу, що заважає вашій здатності виконувати ретельну роботу з оцінки та зменшення ризику. З цієї причини багато організацій звертаються до програмного забезпечення для кібербезпеки, щоб допомогти їм краще оцінити, пом’якшити та контролювати свої стратегії управління ризиками. Сучасні рішення для кібербезпеки розроблені, щоб запобігти трьом основним категоріям ризиків кібербезпеки: зловмисному програмному забезпеченню, програмі-вимагачі та фішингу.

Переваги виконання оцінки ризиків безпеки. Виконання оцінки ризиків кібербезпеки та впровадження процесу управління ризиками у організації має наступні переваги.

1. Зменшує витрати, пов’язані з інцидентами безпеки. Ви можете зменшити довгострокові витрати, пов’язані зі збитками, спричиненими порушенням даних або крадіжкою критичних активів.

2. Забезпечує базовий рівень для організаційного ризику. Він забезпечує базову лінію для майбутніх оцінок, коли ви вирішуєте свій рівень ризику з часом.

3. Підтримує потребу в програмі кібербезпеки. Проведення оцінки ризику надає вашому CISO докази необхідності програми кібербезпеки, яку він або вона може потім показати зацікавленим сторонам.

4. Уникає злому даних. Ви можете виявити загрози, пом’якшити їх і уникнути злому даних.

5. Зменшує проблеми із дотриманням вимог. Можна уникнути проблем із дотриманням нормативних вимог, пов’язаних із даними клієнтів.

6. Зменшує втрати продуктивності. Виявивши вразливі місця та пом’якшивши їх, можна уникнути збоїв, які можуть призвести до втрати продуктивності.

7. Зменшує втрати даних. Крадіжка важливих інформаційних активів може коштувати більше, ніж просто грошові збитки. Розроблений алгоритм ґрунтується на оцінці ризику, який починається з розуміння та узгодження бізнес-цілей із цілями інформаційної безпеки.

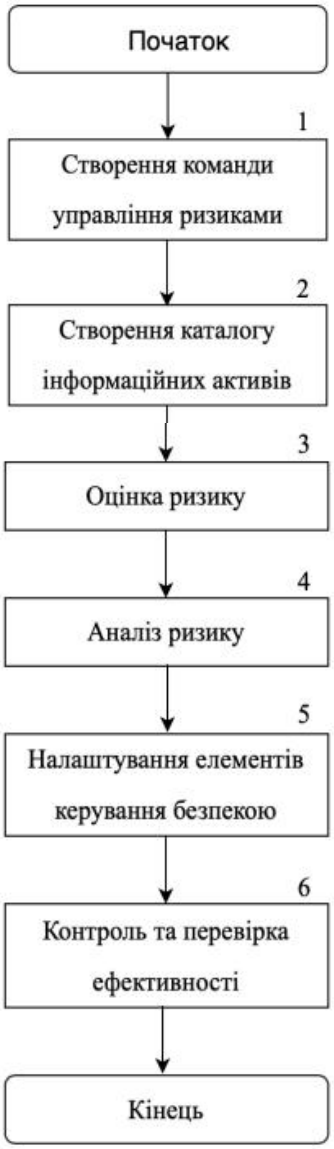

Рис. 1.

Висновок

У сучасному світі, де кібербезпека стає все більш важливою, кожна організація повинна мати свою власну стратегію управління ризиками. Стандарти та нормативні вимоги визнають необхідність різних підходів до захисту інформаційних систем, а комплексна програма захисту інформаційних технологій є ключовою для захисту даних від кіберзлочинності.

Оцінка ризиків кібербезпеки є важливою складовою стратегії управління ризиками, особливо для організацій з IT-інфраструктурою. Незважаючи на обмеження бюджету або робочої сили, багато компаній звертаються до програмного забезпечення для кібербезпеки, щоб допомогти їм краще оцінити, пом'якшити та контролювати свої стратегії управління ризиками.

Переваги виконання оцінки ризиків безпеки включають зменшення витрат, базовий рівень для організаційного ризику, підтримку програми кібербезпеки, уникнення злому даних, зменшення проблем із дотриманням вимог, втрат продуктивності та даних. Важливо, що розроблений алгоритм оцінки ризику ґрунтується на розумінні та узгодженні бізнес-цілей з цілями інформаційної безпеки, що допомагає забезпечити ефективний захист від кіберзагроз.

Список використаних джерел:

1. Хмелевський Р. Дослідження оцінки загрози інформаційної безпеки об’єктів інформаційної діяльності / Р. Хмелевський // Сучасний захист інформації. 4, стор. 65–70, 2016.
2. ISO 31010 2019. Risk management - Risk assessment techniques. Managemensdu risque - Techniques. - 268 p.
3. Akinrolabu O. Nurse J.R., Martin A., New. S. Cyber risk assessment in cloud provider environments: Current models and future needs. Computers & Security, 2019. 87. 101600.
4. Корнієнко Б. Я. Прикладні програми управління інформаційними ризиками / Б. Я. Корнієнко, Ю. О. Максімов, Н. М. Марутовська // Захист інформації. — К. : Науково-практичний журнал, 2012. — Вип. 4. — С. 60–64.